Banking Ombudsman Scheme | Te Whare Rama Tōkeke

Practice note: Fraud and scams

30 November 2025

Purpose

To give guidance on how to investigate complaints about fraud losses to ensure fair customer outcomes. At the Banking Ombudsman Scheme, we aim to help consumers with complaints about banks. We have published this guidance, or fraud practice note, to outline how we approach fraud and scam-related complaints. It is based on our experience in resolving complaints and aims to provide practical information. Note that each complaint we receive is unique, so this document is a guide only.

Introduction

Fraud and scam losses are a problematic area for banks and their customers. When customers suffer such losses, they may expect their bank or the bank that received the fraudulent payment to reimburse them on the basis the bank did not prevent their loss. Banks will usually have played no part in the fraud which caused the loss, and a bank's responsibility to reimburse customers depends on the circumstances and the nature of the fraud.

We can consider complaints that a bank has failed to meet its legal or Code-based obligations or has failed to provide services in accordance with good industry practice.

The Code of Banking Practice (the Code) provides a commitment from banks to reimburse *unauthorised* transactions unless the customers have disqualified themselves from this protection. This commitment applies even where the bank did not contribute to the fraud loss.

The Code also provides a commitment from banks to compensate eligible customers for *authorised* transactions in certain circumstances from 30 November 2025.[1] This applies if the bank has failed to meet the applicable scam protection commitments in the Code and the customer has taken reasonable care.

Banks also have obligations under the Code to act fairly and reasonably, to communicate clearly and effectively and to keep the ways a customer banks secure.

This practice note sets out key issues for banks to consider when assessing a customer's claim for reimbursement to help banks reach the right decision.

[1] Amendment to the Code of Banking Practice to address fraud and scam payment protections and compensation (to apply from 30 November 2025)

Table of contents

Getting the full story early

Responding to the initial report

Once a customer has notified their bank of details that suggest that a fraud has taken place, a bank should take steps as soon as reasonably practicable to identify all fraudulent transactions, prevent any further customer losses (for example, by suspending account access) and attempt to recover the funds (see also Recovering funds).

To properly determine liability for reimbursement, it is crucial to get the full story early. The time when a customer first reports a fraud is when they will have the clearest memory of what happened and how they responded. The best way to capture the report in the customer's own words is to speak with them over the phone at the earliest opportunity – even where the fraud was reported in writing. Avoid any interruptions to give the customer the best opportunity to explain what happened. This information can be very useful in determining the outcome of any fraud investigation and/or complaint, so recording the call can be helpful.

Interviewing the customer

At the earliest possible stage, gather, at a minimum, the following details from the customer:

- the circumstances leading to up the fraud
- the fraudster's explanations for any actions the customer was induced to take
- the extent of the customer's understanding of the technology used to carry out the fraud
- how the payments were made and by whom (the customer or the fraudster)
- how any extra authentication measures (2FA), were used and by whom, if applicable
- what alerted the customer to the fact this was fraud.

Gathering information and evidence

To understand how the fraud took place:

- retrieve, retain and review bank records about how the fraud occurred (for example, logs showing the IP address used to access the customer's internet banking)
- verify the use of 2FA, if applicable
- collect documentary evidence from the customer (for example, correspondence between the customer and fraudster, police acknowledgement form, hospital reports, phone logs, tech report for the device used)
- seek the customer's permission to request information from third parties (for example, the police or the customer's telecommunications provider) if necessary
- liaise with the recipient bank and/or police in New Zealand about the payment, if appropriate.

Bank obligations

When we consider a complaint about fraud losses, we consider what is fair in all of the circumstances having regard to the law, the Code and the principles of good industry practice. Banks have a duty to follow a customer's instructions. However, banks must exercise reasonable care and skill in providing banking services (see section 28 of the Consumer Guarantees Act 1993), and are required to comply with the principles of good industry practice. Banks are also required by the Code to keep customers' information, and how they bank, secure, and to meet the outlined fraud and scam commitments.

In the case of both authorised and unauthorised transactions, banks should consider whether these duties were fulfilled.

Keeping the ways customers bank secure

Under the Code, banks commit to keep their banking systems and the way customers bank secure.

When a bank has not required extra authentication measures for a transaction, it should consider:

- whether it is standard industry practice to use an extra authentication measure for such a transaction
- whether the bank offered different extra authentication measures, and whether it explained the risks and benefits to the customer so he or she could make an informed choice.[2] Such a choice usually involves a trade-off between the convenience of fewer measures versus the security of more measures
- whether the customer had previously opted out of extra authentication measures, and in particular:
    - whether the bank adequately explained the implications of opting out
    - whether the circumstances of the transaction had changed to the extent that the bank should have offered to reinstate extra authentication measures.[3]

In cases where the extra authentication or security measures fall short of industry standards, a bank may be liable for the full loss if the loss wouldn't have otherwise happened.[4]

Where a bank has given inadequate information about extra authentication measures, it may be liable to compensate the customer for having been deprived of the opportunity to safeguard him or herself against fraud. However, the bank may not be liable for the full loss because it is often difficult to say whether better information would have prevented the loss.[5]

[2] Case note 57498
[3] Case note 51751
[4] Case notes 83457, 72745, 89802
[5] Case note 57498

Technological developments may allow banks to introduce more powerful and effective authentication measures. Banks should ensure they keep up to date with technological developments and industry standards on authentication measures.

Good industry practice

There is a good industry practice obligation on banks to act, if the facts and circumstances at the time suggest a real possibility of fraud. Banks should identify and act on indicators of fraud for both authorised and unauthorised transactions, including where a customer's description of the purpose of a transaction suggests a real possibility the customer is being defrauded. This obligation is outlined further below.

Authorised transactions

In many scams, customers themselves send funds to the scammer because they have been deceived about the purpose of the transaction or the identity of the recipient.

Code commitments

Banks have committed in the Code to compensating eligible customers for some or all of their losses when banks have not met their scam protection commitments. The bank should initially assess whether the customer meets the requirements for eligibility under the Code.

Eligibility

An eligible customer is someone who:

- was a consumer using banking services[6]
- made a domestic payment to a New Zealand bank account on or after 30 November 2025
- wasn't using a third-party payment service to make the payment
- wasn't buying goods or services on a social media or online marketplace
- wasn't dishonest or fraudulent
- reported the scam to the Police and their bank within three months of discovery and 12 months of the last payment
- cooperated and responded quickly to the bank's reasonable information requests about what happened.

Customer acting dishonestly or fraudulently

To act dishonestly, a customer must undertake an action that is dishonest and also know it is dishonest. A customer is not dishonest by virtue of being unwittingly caught up in fraud and being unaware of the effect of his or her actions.

[6] As defined in the Consumer Guarantees Act, section 2 – essentially that the services were "of a kind ordinarily acquired for personal, domestic, or household use or consumption".

To act fraudulently, a customer must intentionally undertake an action which involved the use of deliberate deception or misrepresentation to obtain a benefit or advantage. There is a high bar for a bank to be satisfied that a customer has acted dishonestly or fraudulently.

Customer cooperating and responding quickly

Customers need to provide relevant information about what happened. When making reasonable requests for this information, and assessing whether the customer has failed to cooperate or respond quickly to such requests, banks must act fairly, reasonably and in an ethical way.

Whether a customer has cooperated and responded quickly to the bank depends on all of the circumstances. In assessing the customer's responses, banks should be aware that following the discovery of authorised transaction fraud, customers may be upset and embarrassed, feel suspicious and have difficulty trusting the bank. When appropriate, banks should explain to the customer their obligation to cooperate and respond quickly in order to be an eligible customer under the Code.

Scam protection commitments

The scam protection commitments outlined in the Code are to:

(1) Provide specific education warnings to consumers before certain payments are made

- Ask customers to confirm their payment purpose
- Based on the information provided, banks will, when appropriate, provide specific education warnings for known high-impact scam types to help consumers identify and avoid them (for example, investment scams)

(2) Provide a Confirmation of Payee service

- Offer a service to consumers for retail mobile and web banking channels to check the name of the person a customer is paying matches the account name
- Provide clear information about how the service works and the risks of making a payment if the customer did not receive a 'match', including where the service cannot confirm the account name for any reason.

(3) Identify high-risk transactions and respond appropriately

- Have policies and processes to identify and respond to the risk of scams
- Help protect customers against high-risk transactions, and banks may use questions or real-time warnings, or delay or block transactions, among other things
- Train frontline staff about common scams, how to keep banking safe, and to respond appropriately where there are clear warning signs a customer may be getting scammed
- Not all transactions will be 'high risk'. They may include large payments, multiple payments to the same person over a short time, or certain payment types

(4) Provide a 24/7 reporting channel for customers and respond to reports of a scam within a reasonable timeframe

- Provide clear information about what to do if a customer thinks they have been scammed, including how to stop electronic banking or block their cards, and banks will provide 24/7 options to report scams
- Act quickly to protect a customer's banking, and investigate and seek to recover money in a reasonable timeframe

(5) Share information with other banks to help prevent criminal activity and to freeze funds where appropriate.

- Share data and information with other banks to help prevent scams and recover money faster
- Act on that scam intelligence in a timely manner, stopping payments and closing accounts identified as mule accounts where appropriate
- Work with the receiving bank to attempt to recover the funds

We recognise that banks will carefully assess the particular circumstances when considering what steps may be reasonable upon receiving 'scam intelligence' about a customer's account – including any vulnerabilities.

Whether customer took reasonable care

In deciding whether to compensate eligible customers for all or some of their loss, banks may consider whether the customer took reasonable care when deciding to make or making the payment.

Other duties

A bank may also be liable for some or all of the losses if it has failed to meet its legal or other Code-based obligations or has failed to provide services in accordance with good industry practice. For example, if:

- the bank failed to comply with the customer's instructions (for example, mistakenly paid the funds into the wrong account)
- the bank's terms and conditions undertake to reimburse such losses (for example, if the terms and conditions provide for a general reimbursement for "fraud losses").[7]

On notice customer may be being scammed

A bank has a strict duty to follow a customer's transaction instructions. However in carrying out the customer's instructions, a bank must act with reasonable care and skill and in accordance with good industry practice.

[7] Case note 60959

Good industry practice requires that if a bank detects (or ought to have detected) warning signs of a real possibility that a customer is being scammed or defrauded (so-called "red flags"), it should act. A bank cannot ignore indications of a possible scam.

When a bank is on notice of a real possibility that the customer may be being scammed or defrauded, good banking practice requires it to make inquiries or warn the customer. Loading a warning on the customer's profile, filing a suspicious transaction report or declining to act on the customer's instructions may be appropriate in some circumstances.

It is not possible to provide an exhaustive list of warning signs or "red flags" but indicators may include:

- The customer is unable to explain the purpose of the transaction, or provides confused or conflicting information.
- The customer's description of the purpose of the transaction has one of the hallmarks of common types of scams, such as the funds are for an online romantic partner, are intended to release an inheritance, or are needed for an investment that will be sent via another account.
- The bank is aware that a third party is likely exerting undue influence over the customer.[8]

A bank may be liable for some or all of a customer's losses if it has failed to act when on notice of a real possibility a customer is being scammed or defrauded.[9] However, a bank is unlikely to be liable if it was not on notice,[10] or a customer decided to proceed with the transaction despite the bank's warning.[11]

Unauthorised transactions

There can be no authority to transfer funds if a customer does not provide instructions to process the payment. In such a case, the Code requires that a bank reimburse the customer unless it can demonstrate, on the balance of probabilities, that the customer:

- was dishonest or negligent, or
- did not take reasonable steps to protect his or her banking or
- did not cooperate and respond quickly to reasonable requests for information about what happened.

Note that the burden of proof is on the bank to show that the customer more likely than not disqualified themselves. The bank should identify the applicable ground for disqualification and explain to the customer how his or her actions met that ground for disqualification.

[8] Australian Financial Complaints Authority determination case 526362
[9] Case notes 44313, 82762, 83106, 88556
[10] Case notes 84271, 87525, 88446, 90352
[11] Case notes 74303, 77946, 87401

Customer disqualification

Dishonesty

As noted above, to act dishonestly, a customer must undertake an action that is dishonest and also know it is dishonest. A customer is not dishonest by virtue of being unwittingly caught up in fraud and being unaware of the effect of his or her actions.

Negligence or failure to take reasonable steps to protect banking

The Code states customers are disqualified from reimbursement if they have acted negligently or not taken reasonable steps to protect their banking. These are two ways of expressing that customers must observe a reasonable standard of care.

Reasonable care is an objective standard so banks should look at what a reasonable person would have done in the customer's situation and whether this differs from how the customer acted. The fact that a customer fell victim to fraud, disclosed information and/or allowed the use of remote access software does not, in itself, mean the customer failed to take reasonable care.[12]

Keep in mind that a reasonable person is an average person, not a banker, and has only the same degree of knowledge of the surrounding events as the customer in question had.

Consider each action the customer took that contributed to the loss, including:

- what the customer did, and why
- what a reasonable person would have done in such a scenario
- whether there is any difference between what the customer did and what a reasonable person would have done.

As these factors are highly contextual, negligence assessments should be done on a case- by-case basis. Even where fact scenarios leading to fraud losses are very similar, there may be other factors (for example, the customer's knowledge or understanding of the events) which result in different conclusions on whether the customer took reasonable care. [13]

When communicating with customers, it may sound harsh or critical to say that they have been negligent. The customers may respond better if it is explained that they have not shown a reasonable standard of care.

Failure to cooperate and respond quickly

As noted above, customers need to provide relevant information about what happened. When making requests for this information, and assessing whether the customer has failed to cooperate or respond quickly to such requests, banks must act fairly, reasonably and in an ethical way.

---

[12] Case note 92261, 93129

[13] See case note 51751 where using remote access software wasn't negligent, and case note 52330 where it was.

Whether a customer has cooperated and responded quickly to the bank depends on all of the circumstances. In assessing the customer's responses, banks should be aware that following the discovery of fraud, customers may be upset and embarrassed, feel suspicious and have difficulty trusting the bank. When appropriate, banks should explain to the customer their obligation to cooperate and respond quickly under the Code.

Phishing scams

In phishing scams, scammers may impersonate a legitimate organisation and will usually send an unsolicited email or text message containing a link to an imposter website.

Phishing messages and imposter sites are often extremely convincing. We do not generally consider clicking on links in emails or text messages alone to be negligent, and nor do we consider that customers should have realised that a website was fake unless there were clear warning signs that should have alerted a reasonable person to the likelihood of a scam.

Clear warning signs may include:

- a text from an organisation seeking banking information or a payment when the customer would not reasonably expect such a request, for example a text to pay a car registration when the customer had no car
- a very low standard of presentation or content (such as amateurish design or bad grammar) in a message and/or imposter website
- a scam that is well known and well publicised, especially if a customer has received a recent notification direct from the bank about a specific scam.

When assessing a phishing scam complaint, we will consider all of the circumstances at the time, including the level of public awareness of the scam and whether the person was expecting contact from the relevant agency.

Many recent phishing scams involve impersonation of banks or government departments and can involve phishing two-factor authentication (2FA) codes as well.

Bank impersonation phishing scams

These scams can take the following forms:

- Customers use a search engine to find their bank and click on a result that appears to be their bank website. They are taken to a fake bank internet banking log-in page where they enter their internet banking credentials.
- Customers receive a text message or email purporting to be from their bank that warns of some new or suspicious activity on their account and asks them to click on a link in response. In clicking on the link, customers are redirected to what appears to be the bank's internet banking log-in page where they enter their internet banking credentials.

- Customers receive a call from someone purporting to be from their bank, often the bank's fraud team. The caller will usually have already information about the customer, such as personal information and credit card details. Texted codes are then obtained from the customer under the guise of protecting their account or reversing transactions.

Whether a customer has acted negligently needs to be considered in the specific circumstances of each case. If the log-in page contains no obvious warning signs that it is not authentic, we generally do not consider it negligent for customers to enter their credentials into what they reasonably believed to be their bank's website.

Where a customer has shared codes with someone they reasonably believe to be their bank, the customer may not have acted negligently, particularly where the customer has taken steps to verify it is their bank.[14] A customer may have acted negligently by giving the caller credit card details as well as codes, or by not acting on suspicions about a caller's identity.[15]

Government department impersonation phishing scams

These scams can take one of the following forms:

- Customers receive an email purportedly from the Inland Revenue Department saying a *refund is available* and directing them to click on a link to enter their bank account details. They are taken to a drop-down list of banks from which they select their bank and enter their internet banking credentials.
- Customers receive an email or text message purportedly from Waka Kotahi NZ Transport Agency *asking for payment* of a toll or vehicle registration. The email or text contains a link to make the payment. Customers are redirected to a card payment page and enter their card details.
- Customers receive an email or text message purportedly from NZ Post (or another courier service) about a parcel delivery and are directed to click on a link to pay a *redelivery fee*. They are taken to a card payment page where they enter their card details.

If there are no warning signs that should have alerted a reasonable person to the likelihood of a scam, we generally do not consider it negligent for customers to enter their bank credentials to authorise payments or refunds.[16]

Phishing two-factor authentication codes

In some phishing scams, scammers need to obtain 2FA codes to succeed in their scam. They can use these codes to:

- authorise a payment initiated from a customer's bank account or credit/debit card
- finalise the installation of a bank's mobile app or digital wallet (such as

[14] Case notes 81162, 87834, 88314, 88454
[15] Case notes 82803, 87981
[16] Case notes 78531, 81682, 90793

GooglePay or ApplePay) on a new device.

Whether a customer caught up in a phishing scam has taken reasonable care depends on the facts and circumstances of each case. Banks should therefore take care if using standard template responses to reimbursement requests.

In considering what is reasonable care of verification codes, banks should remember it is standard practice these days to enter a code and people are conditioned to enter codes when prompted. Banks should keep in mind that the fact an authentication code has been used does not necessarily mean a customer has disclosed the code or failed to take reasonable care.

Text messages accompanying the codes should be sufficiently clear about what the code is being used for. A text message should clearly state what action the code will allow, such as to make a payment or change a password. For transactions, the message should include the payment amount, currency and recipient. The message should ideally include instructions on where to enter the code (for example, in internet banking, in the banking app or on the merchant's website) and what customers should do if they did not request the code.[17] Banks should avoid jargon or ambiguous terms such as "to activate the app" or "to validate and continue your action".

If a bank sends a customer a verification code for a payment to a specified recipient for a specified amount, and the customer enters it without understanding they were approving the payment, the payment is still considered unauthorised. However, if the customer fails to read the message or ignores a clear warning, we will generally consider the customer has acted without reasonable care.[18]However if there are no warning signs that should have alerted a reasonable person to the likelihood of a scam, we may conclude the customer did not act negligently.

If a verification code has been used but the customer says they didn't enter it, banks should keep an open mind to the possibility that the code was entered without the customer's knowledge.[19] Some phishing links contain malware enabling scammers to access information on a customer's device. Also, features on mobile devices can automatically enter a code into a website without a customer needing to open a message. When a customer reports not having received a text message with a code, a bank should make enquiries about whether the device has been compromised.

A bank's liability under the Code is unaffected by whether it can recover a payment via a chargeback or other recovery method. Even if a chargeback is not available, a bank may nonetheless be liable under the Code.

Recovering funds

Banks must take reasonable steps when alerted that a payment may have been made as part of a scam, including taking steps to attempt to recover the funds within a reasonable timeframe. Like all banking services, this must be done with reasonable care and skill. In many cases, the bank is a customer's only way to try to recover funds, and any delay can allow the recipient to

[17] Case note 88457
[18] Case note 84423
[19] Case note 93129

withdraw the funds first.

For credit card transactions, the bank should consider whether there are any available chargeback grounds under the credit card provider's rules.

Most frauds involve payments made using internet banking and recovering the funds will involve the paying bank contacting the receiving bank to ask for the funds to be returned. If a paying bank fails to initiate the recovery process within a reasonable timeframe, it will be liable for any loss resulting from its delay.[20] If the funds have already left the receiver's account by the time the customer raises the alert, any delay by the bank will not have any practical consequence because the funds are unrecoverable. However, banks should consider whether compensation for distress is warranted in such circumstances.[21] If some or all of the funds could have been recovered if the bank acted within a reasonable timeframe, the bank may be liable for the amount that could have been recovered.[22]

If the bank did not take steps within a reasonable timeframe, the burden is on a bank to show that, on the balance of probabilities, its delay did not contribute to its inability to recover the funds. The receiving bank can usually provide information about when the funds left the receiving account.

Receiving banks should contact a customer who has received fraudulently obtained funds as soon as possible about the return of the funds. Where a customer has received fraudulently obtained funds into their account, the receiving bank must treat their customer fairly and reasonably, as well as communicate with them clearly and effectively. Banks need to ensure that action taken against such customers (who may be innocent of any wrongdoing) is fair, consistent and provided for in the terms and conditions of a customer's account.

It will generally be reasonable for a bank to invoke a clause in its terms and conditions that allows it to reasonably suspend an account or otherwise freeze the relevant funds, at least for a period. However, it cannot do so indefinitely. Banks ought to have processes in place to end such a freeze (and direction may be needed from police and/or the courts). We expect the bank to clearly communicate this process to its customer.[23]

If the customer has already spent or withdrawn the money before the bank is aware of a third party's claim, the bank must act fairly and in accordance with its contract with the customer.[24]

Fair and reasonable outcomes

Banks must treat customers fairly and reasonably, and what is fair and reasonable depends on the circumstances including the customer's conduct, the bank's conduct, the terms and conditions, the law and good industry practice.

In some cases, there may be compelling circumstances beyond the legalities of liability which

[20] Case note 54681
[21] Case notes 55433, 74040
[22] Case note 52330
[23] Case note 95895
[24] Case note 84279

suggest it would be fair and reasonable for the bank to compensate the customer.[25] Examples include where the customer is vulnerable or suffering financial hardship, or where the bank has met minimum conduct standards but fallen below its own service expectations. While such circumstances may not warrant full reimbursement, the bank should consider whether apportionment of the loss may be appropriate.

Communicating reimbursement decisions

A bank should relay its decision about a customer's fraud reimbursement claim with empathy and sensitivity, and within a reasonable time. Decisions on reimbursement claims should in most cases be communicated within 20 working days.

Poor communication can needlessly cause or draw out complaints. This is frequently a key factor in a customer's decision to engage a lawyer and fight a bank's decision. Banks should give clear reasons for their decision. Banks may have to pay compensation for poor service, such as inadequate communication, even if they are not liable to reimburse fraud loss.[26]

[25] Case note 57498

[26] Case note 60959